Homework 4

There are two Gradescope submissions for this assigment, one PlayCrypt code and one short-answer. This PDF is being given out so that you can see what the problems look like in mathematical notation, but you do not need to submit a PDF anywhere.

We suggest that you start with this version. Work out a solution using pencil and paper. Move to implementation in PlayCrypt only after that.

As usual our convention is that the running time of an adversary does not include the time taken by game procedures to compute responses to adversary queries.

Note: This problem set is due after the midterm. We strongly suggest understanding the topics prior to the midterm.

Problem 1 [10 points] Alice wants to send Bob a file, but she's worried that someone might tamper with the file as it travels over the network. To protect the file against unauthorized modification, Alice uses an IND-CPA secure encryption scheme (like AES-CTR or AES-CBC) to encrypt the file before sending it, using a key that Alice and Bob both already know. Is this sufficient? If not, what should Alice do instead?

Submit your answer in **no more than two sentences** on the Gradescope assignment "Short Answer 4."

Problem 2 [50 points] Let $E\colon \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a block cipher and let T_E denote the time to compute E or E^{-1}. Let D be the set of all strings whose length is a positive multiple of l, meaning:

$$D = \{\, M \in \{0,1\}^* \,:\, |M| > 0 \text{ and } |M| \bmod l = 0 \,\}\,.$$

In the pseudocode below, $M[1]M[2]\ldots M[n] \leftarrow M$ means we break M into l-bit blocks, with $M[i]$ denoting the i-th block and n the number of blocks.

Define the hash function $H_2\colon \{0,1\}^k \times D \to \{0,1\}^l$ as follows:

Alg $H_2(K, M)$
$M[1]M[2]\ldots M[n] \leftarrow M$
$C[0] \leftarrow 0^l$
For $i = 1, \ldots, n$ do $W[i] \leftarrow E(K, C[i-1] \oplus M[i])$; $C[i] \leftarrow E(K, W[i] \oplus M[i])$
Return $C[n]$

Show that H_2 is not collision-resistant by presenting an $\mathcal{O}(T_E{+}l)$-time adversary A_2 with $\mathbf{Adv}^{\mathrm{cr}}_{H_2}(A_2) = 1$. Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment "Problem Set 4."

Problem 3 [50 points] Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with $n \geq 4$. Let

$$D \;=\; \{\, M \in \{0,1\}^* \,:\, 0 < |M| < n2^n \text{ and } |M| \bmod n = 0 \,\}\,.$$

Let $\mathcal{T}\colon \{0,1\}^k \times D \to \{0,1\}^n$ be defined as follows:

Alg $\mathcal{T}_K(M)$
$M[1]\ldots M[m] \leftarrow M$; $M[m+1] \leftarrow \langle m \rangle$; $C[0] \leftarrow 0^n$
For $i = 1, \ldots, m+1$ do $C[i] \leftarrow E_K(C[i-1] \oplus M[i])$
$T \leftarrow C[m+1]$; Return T

Above, $M[1]\ldots M[m] \leftarrow M$ means we break M into n-bit blocks, and $\langle m \rangle$ denotes the n-bit binary representation of the integer m. (For example, if $n = 8$ and $m = 2$ then $\langle m \rangle = 00000010$.)

Show that $\mathcal{T}$ is an insecure message-authentication code by presenting an $\mathcal{O}(n)$-time adversary A, making at most 2 queries to its **Tag** oracle, and achieving $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{T}}(A) = 1$. Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment "Problem Set 4."
